KECS-CR-08-54

WEBS-RAY V2.5 인증보고서

인증번호 : KECS-NISS-0137-2008

2008년 12월

IT보안인증사무국

제·개정 이력 현황

개정 번호	제·개정일	개정쪽	제·개정내용
00	2008.12.22	-	최초 작성

본 문서는 (주)트리니티소프트의 WEBS-RAY V2.5에 대한 인증보고서이다.

인증위원

행정안전부 장영환, 국가보안기술연구소 윤이중, 고려대학교 이희조,
광운대학교 유황빈, 성균관대학교 원동호, 숭실대학교 이경석,
한양대학교 송정환, 한국전자통신연구원 손승원, 한국정보보호학회 이홍섭

인증기관

IT보안인증사무국

평가기관

한국정보보호진흥원

목 차

1. 요약

본 보고서는 WEBS-RAY V2.5에 대한 정보보호시스템 공통평가기준(2008년 7월 16일 고시)(이하 '공통평가기준'이 한다) EAL4 평가결과에 대한 인증기관의 인증결과를 서술한다. 본 보고서는 평가결과, 평가결과의 타당성 및 적합여부를 서술한다.

WEBS-RAY V2.5에 대한 평가는 한국정보보호진흥원에서 수행되었으며, 2008년 12월 5일에 평가 완료되었다. 본 보고서의 내용은 한국정보보호진흥원에서 제출한 평가보고서의 내용에 기초하여 작성되었다. 평가는 제품이 공통평가기준 2부와 3부의 EAL4 평가보증등급을 만족하여, 공통평가기준 1부 191항에 따라 "적합"한 것으로 평가하였다.

WEBS-RAY V2.5는 웹 서버에 대한 서비스 공격을 탐지 및 차단하기 위하여 White URL을 설정하여 웹에서 발생할 수 있는 공격들을 탐지하여 차단하는 기능을 제공하는 소프트웨어 기반의 웹 어플리케이션 방화벽 제품으로 (주)트리니티소프트에서 개발되었다.

WEBS-RAY V2.5은 웹 공격에 대한 탐지 및 차단 기능을 수행하는 Agent, 보안정책을 관리하고 감사기록을 저장하는 Master Server, 보안정책 설성 등 보안관리를 위해 관리자에게 GUI를 제공해 주는 Admin Console로 구성된다. 평가제품은 아래와 같은 주요 보안기능을 제공한다:

- 인가된 관리자에게만 허용되는 보안관리 기능
- 보안감사 데이터의 생성 및 보호 기능
- 보안정책에 따라 웹 공격을 탐지 및 차단하고, 웹 컨텐츠를 보호하는 사용자 데이터 보호 기능
- 외부 IT 실체에 대한 식별 및 인가된 관리자에 대한 식별 및 인증기능
- TSF 실행파일 및 보안정책에 대한 무결성을 점검하고, 주기적으로 TSF 서비스 데몬 및 통신채널에 대한 정상 동작을 확인하는 시스템보호 기능

인증기관은 평가자의 평가활동 및 시험절차를 점검하고, 기술적인 문제점 및 평가절차에 대한 지침을 제공하고, 각 평가단위 및 평가보고서의 내용을 검토하였다. 인증기관은 평가제품이 보안목표명세서에 서술된 모든 보안기능 요구사항 및 보증요구사항을 만족함을 평가결과가 보증함을 확인하였다. 따라서, 인증기관은 평가자의 관찰사항과 평가결과가 정확하고 타당하며, 적합여부 평가결과가 정확하다고 인증하였다.

인증 효력범위 : 본 인증보고서에 포함된 정보는 WEBS-RAY V2.5이 대한민국 정부기관에 의한 사용 승인 또는 WEBS-RAY V2.5에 대한 품질보증을 의미하지 않는다.

2. 식별정보

다음 [표 1]은 평가제품 식별을 위한 정보를 나타낸다.

[표 1] 평가제품 식별정보

평가지침	정보보호시스템 평가·인증지침 (2008. 7. 16.) 정보보호제품 평가인증 수행규정 (2008. 9. 1.)
평가제품	WEBS-RAY V2.5
보호프로파일	해당없음
보안목표명세서	WEBS-RAY V2.5 보안목표명세서 V2.8 (2008. 11. 3.), (주)트리니티소프트
평가보고서	WEBS-RAY V2.5 평가결과보고서, 발행버전 1.0 (2008. 12. 5.)
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V2.3 (2008. 7)
평가방법론	정보보호시스템 공통평가방법론 V2.3 (2008. 7)
평가신청인	(주)트리니티소프트
개발업체	(주)트리니티소프트
평가자	한국정보보호진흥원 보안성평가단 오용석, 유희준
인증담당자	IT보안인증사무국

WEBS-RAY V2.5의 시스템 운영환경은 [표 2], [표 3]과 같다.

[표 2] WEBS-RAY V2.5(일체형) 시스템 사양

항목			최소사양
GW-1000 일체형	공통	CPU	Intel DuoCore 2.0GHz * 1EA
		Memory	2GB
		NIC	10/100M/1G bps (UTP*6)
		HDD	160GB
		OS	전용 OS (2.5)
	Agent	Proxy Server	Apache 2.2.8
	Master Server	DB	MySQL 4.1
GW-2500 일체형	공통	CPU	Intel QuadCore 2.0GHz * 1EA
		Memory	4GB
		NIC	10/100M/1G bps (UTP*4, Fiber*4)
		HDD	250GB
		OS	전용 OS (2.5)
	Agent	Proxy Server	Apache 2.2.8
	Master Server	DB	MySQL 4.1
GW-3000 일체형	공통	CPU	Intel QuadCore 2.5GHz * 2EA
		Memory	8GB
		NIC	10/100M/1G bps (UTP*4, Fiber*4)
		HDD	250GB
		OS	전용 OS (2.5)
	Agent	Proxy Server	Apache 2.2.8
	Master Server	DB	MySQL 4.1
Admin Console		CPU	Intel Pentium IV 1GHz 이상
		Memory	256MB 이상
		NIC	10/100/1G bps
		HDD	40GB 이상
		OS	Windows XP SP2

[표 3] WEBS-RAY V2.5(분리형) 시스템 사양

항목		최소사양
GW-1000 Agent	CPU	Intel DuoCore 2.0GHz * 1EA
	Memory	2GB
	NIC	10/100M/1G bps (UTP*6)
	HDD	160GB
	OS	전용 OS (2.5)
	Proxy Server	Apache 2.2.8
GW-2500 Agent	CPU	Intel QuadCore 2.0GHz * 1EA
	Memory	4GB
	NIC	10/100M/1G bps (UTP*4, Fiber*4)
	HDD	250GB
	OS	전용 OS (2.5)
	Proxy Server	Apache 2.2.8
GW-3000 Agent	CPU	Intel QuadCore 2.5GHz * 2EA
	Memory	8GB
	NIC	10/100M/1G bps (UTP*4, Fiber*4)
	HDD	250GB
	OS	전용 OS (2.5)
	Proxy Server	Apache 2.2.8
Master Server	CPU	Intel DuoCore 2.0GHz * 1EA 이상
	Memory	2GB 이상
	NIC	10/100M/1G bps
	HDD	160GB 이상
	OS	FedoraCore 6 + Linux Kernel 2.6.20
	DB	MySQL 4.1
Admin Console	CPU	Intel Pentium IV 1GHz 이상
	Memory	256MB 이상
	NIC	10/100/1G bps
	HDD	40GB 이상
	OS	Windows XP SP2

3. 보안정책

평가제품은 아래와 같은 보안정책을 준수하여 운영된다.

보안감사 보안과 관련된 행동에 대한 책임을 추적하기 위해 보안관련 사건은 기록 및 유지되어야 하며, 기록된 데이터는 검토되어야 한다.

안전한관리 인가된 관리자는 안전한 방법으로 TOE를 관리해야 한다.

4. 가정사항 및 범위

4.1 가정사항

평가제품은 아래와 같은 가정사항을 준수하여 설치 및 운용되어야 한다.

A.물리적보안 TOE는 인가된 자만이 접근 가능한 물리적으로 안전한 환경에 위치한다.

A.보안유지 네트워크 구성 변경, 호스트의 구성 변경, 웹 서버의 구성 변경, 웹 애플리케이션의 변경 등으로 보안 환경이 변화될 때, 변화된 환경과 보안정책이 즉시 TOE 운영정책에 반영되어 이전과 동일한 수준의 보안을 유지한다.

A.신뢰된관리자 TOE의 인가된 관리자는 악의가 없으며, TOE 관리 기능에 대하여 적절히 교육 받았고, 관리자 지침에 따라 정확하게 의무를 수행한다.

A.운영체제보강 TOE에 의해 필요하지 않은 운영체제상의 서비스(서비스 포트)나 수단 등은 모두 제거하는 작업을 통해 운영체제상의 취약성을 사전에 제거하여 운영체제에 대한 신뢰성과 안전성이 보장된다.

A.웹서버보강 TOE에 의해 웹 서버상 존재하는 불필요한 프로그램을 제거하고 최신 버전으로 패치하는 등 취약성을 사전에 제거하여 웹 서버에 대한 신뢰성과 안전성이 보장된다.

A.안전한외부서버 TOE의 신뢰성 있는 시간을 유지하기 위하여 NTP 서버로부터 최신 시간을 받아오게 되는데 이 서버에 대한 신뢰성과 안전성이 보장된다.

A.안전한SSL	TOE간 사용할 SSL은 안전하게 운영되고 TOE 간에 전달되는 데이터의 기밀성이 보장된다.
A.안전한DB	TOE에서 생성되는 감사데이터를 안전하게 저장하고 감사데이터의 검색 및 정렬에 사용되는 DB의 안전성이 보장된다.

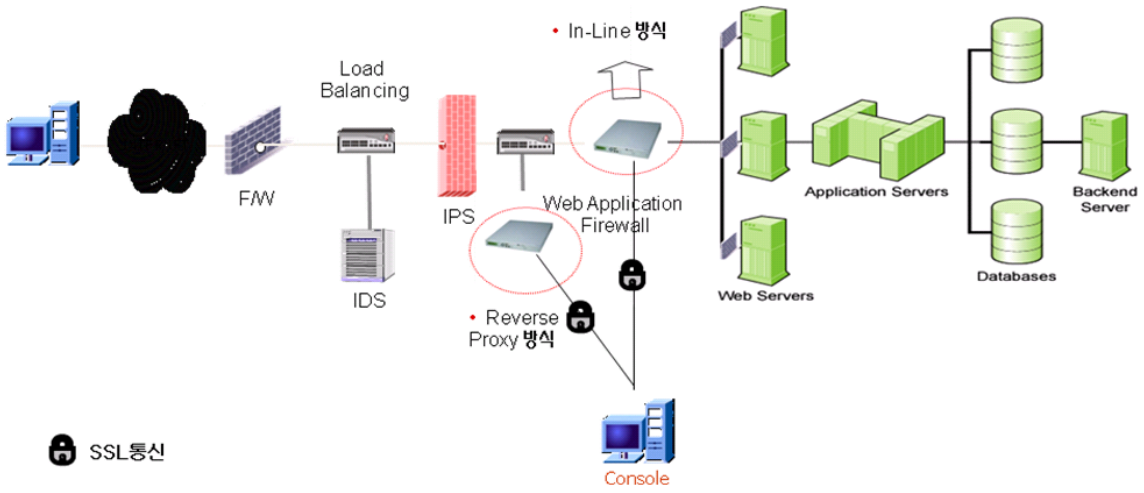
4.2 위협 대응범위

평가제품은 TOE가 요구하는 IT 환경에 적합한 수준의 보안위협에 대한 대처방법을 제공하고 있으며, 평가제품을 비정상적으로 운용되도록 하는 직접적인 물리적 공격에 대한 대처방법을 제공하고 있지 않다. 그러나, 평가제품은 평가제품과 연결된 네트워크에서 낮은 수준의 전문지식, 자원, 동기를 가진 위협원에 의해 발생하는 논리적 공격에 대한 대처방법을 제공한다.

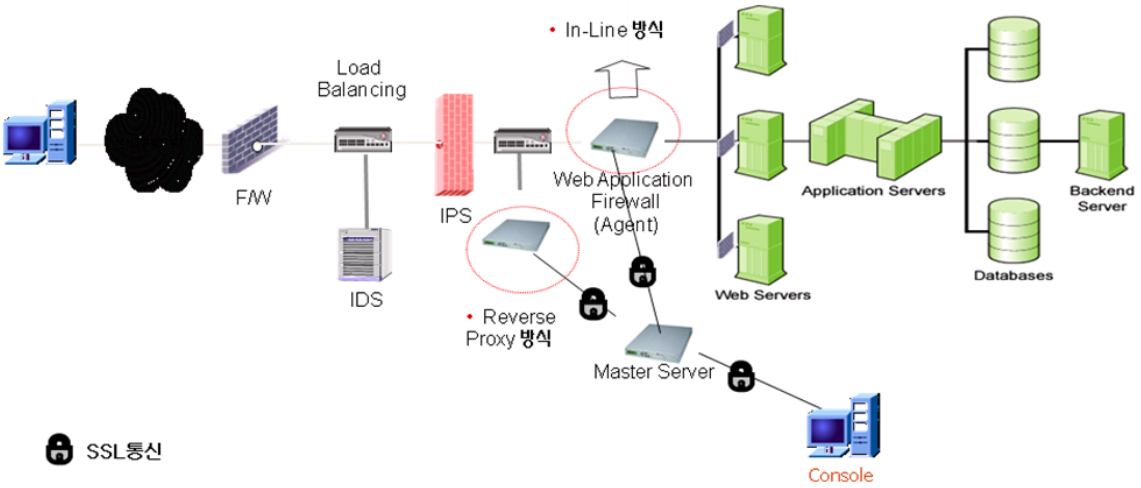
모든 보안목적 및 보안정책은 식별된 보안위협에 대한 대처방법을 제공할 수 있도록 서술되어 있다.

5. 제품정보

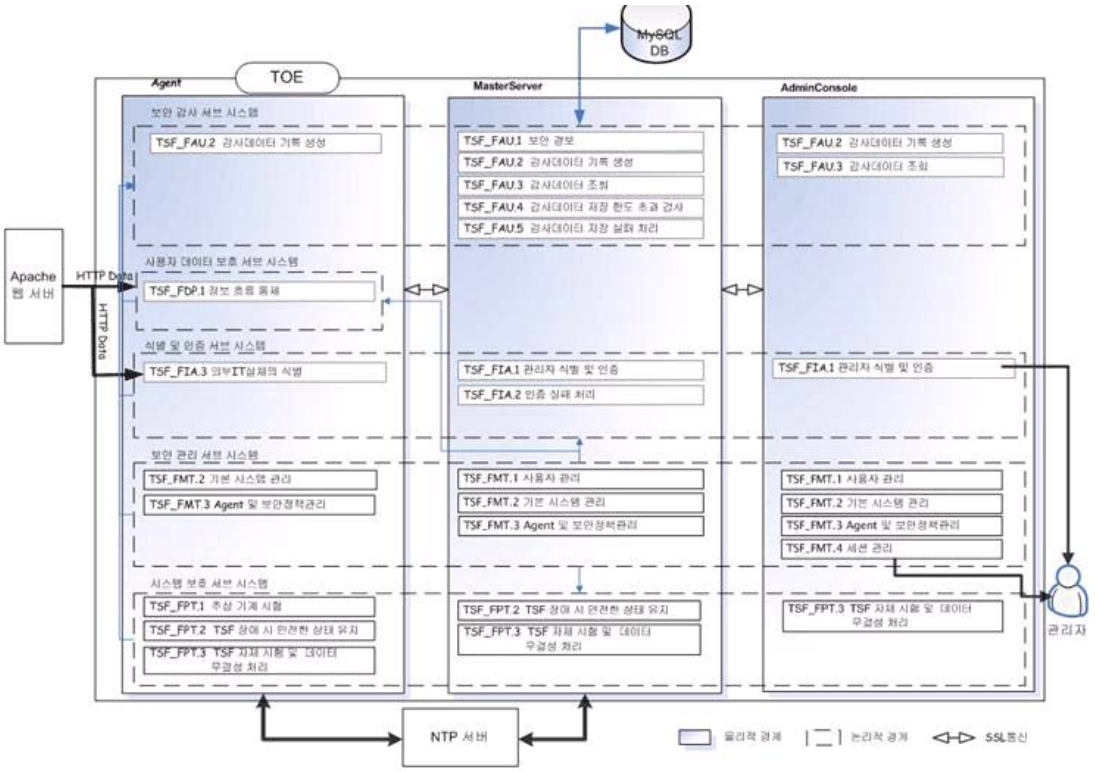
평가제품은 침입차단시스템 등과 같은 네트워크 보안제품에 의해 보호되는 내부망 또는 DMZ에 설치되어 운영되며 운영환경은 [그림 1], [그림 2]와 같으며, 기본구조는 다음 [그림 3]과 같다.



[그림 2] WEBS-RAY V2.5(일체형) 운영환경



[그림 3] WEBS-RAY V2.5(분리형) 운영환경



[그림 4] WEBS-RAY V2.5 기본구조

평가제품은 다음과 같은 5개의 서브시스템으로 구성된다.

- **보안감사 서브시스템(SA)**

각 서브시스템(사용자데이터보호 서브시스템, 식별 및 인증 서브시스템, 보안관리 서브시스템, 시스템보호 서브시스템)들이 생성하는 감사 데이터들을 Master Server로 전송하고 MySQL DB에 저장하여 침입시도 로그, 컨텐츠 변조 로그, 작업 로그, 알림 메세지별로 감사기록 데이터를 확인할 수 있다. 또한 MySQL DB에 저장되어 있는 감사

기록 데이터의 저장 및 포화 한도를 검사하여 기본값으로 지정한 한도를 초과하게 되면 감사기록 저장소의 디스크가 모두 소진한 것으로 인식하고 더 이상 감사기록 정보들이 저장되는 것을 막기 위해서 인가된 관리자의 접속, 백업을 제외한 모든 TSF 서비스를 정지한다.

- **사용자 데이터 보호 서브시스템(UP)**

웹 어플리케이션에 접근하는HTTP(S) 요청 및 사용자 영역으로 전송되는 HTTP(S) 응답에 대하여 침입 및 트래픽 분석 처리를 하고 있으며 이에 대해 우회접근 및 서비스 거부를 방지한다. 만약 비정상적인 공격이 발생되면 해당 공격들을 탐지 및 차단을 하게 되고 비정상적인 접근에 대해서 감사기록을 생성한다. 주요한 컨텐츠 파일에 대해서는 감시 대상으로 등록하고 등록된 파일들에 대해 해쉬값을 저장하여 무결성 점검 주기에 따라 변경 여부를 검사하고 변경시 감사기록을 생성한다.

- **식별 및 인증 서브시스템(IA)**

TOE를 관리하는 관리자에 대해서 식별 및 인증 기능을 수행하고 외부 IT 실체(클라이언트)에 대한 식별을 수행한다. Admin Console에서 제공하는 로그인 페이지를 통해서 관리자의 식별 및 인증 기능을 제공하고 있으며 슈퍼관리자 계정을 제외한 관리자 및 모니터 계정에 대한 접근 실패 횟수, 계정 만료에 대한 인증 설정 내역을 반영한다. 로그인 실패 시 보안관리 서브시스템(SM)으로 실패 사항을 전달한다.

- **보안관리 서브시스템(SM)**

정보 흐름 통제 및 컨텐츠 변조에 대한 정책을 비롯하여 TSF 데이터를 생성하고 변경, 삭제할 수 있는 GUI를 제공한다. 또한 TOE의 TSF의 실행 코드와 각종 보안 정책의 속성 정보에 대한 무결성 점검, TSF 및 TSF 데이터에 대한 정책 설정, 상태 조회, 변경 작업을 수행한다.

- **시스템보호 서브시스템(SP)**

Agent, Master Server, Admin Console의 정상적인 운영 및 안전한 상태를 유지하기 위해 TSF 서비스 데몬 장애, 통신 장애를 구동시 및 정규운영 동안 주기적(30초)으로 확인한다. 데몬의 장애가 발생한 경우 감시 프로세스가 해당 서비스 데몬을 재구동시켜 안전한 상태를 유지하도록 한다. 또한 제어 채널의 상태를 주기적으로 확인하여 제어 채널에 문제가 발생하면 통신 상태 문제로 판단하고 통신이 재개될 때까지 감사기록을 저장한 후 통신이 재개되면 저장된 감사기록을 Master Server로 송신한다. 그리고, TSF의 실행코드, 보안정책파일, 시스템 동작 파일, 보안정책 테이블 파일에 대해 시동시 및 지정된 주기(기본값 5분)마다 무결성 점검을 수행한다. 무결성에 대한 오류 발생시, 설정한 대응 행동 정보에 따라 보안 경보 내역이 인가된 관리자에게 전달되며 관리자는 결과 보기를 통해 무결성 오류에 대한 확인을 수행한다.

6. 설명서

평가제품이 제공하는 설명서는 아래와 같다:

- WEBS-RAY V2.5 관리자설명서 V2.7, 2008년 11월 3일
- WEBS-RAY V2.5 설치지침서 V2.8, 2008년 11월 19일

7. 제품시험

7.1 개발자 시험

- **시험방법**

개발자는 제품의 보안기능을 고려하여 시험항목을 도출하였다. 각 시험항목은 시험서에 서술되어 있다. 시험서에 서술된 각 시험항목은 아래의 세부 항목을 포함하고 있다:

- 시험번호/시험자 : 시험항목 식별자 및 시험에 참여한 개발자
- 시험목적 : 시험 대상 보안기능 및 보안모듈을 포함하여 시험의 목적을 서술
- 시험환경 : 시험을 수행하기 위한 세부 시험환경
- 세부 시험절차 : 보안기능을 시험하기 위한 세부 절차
- 예상결과 : 시험절차를 수행하였을 때 나타날 것으로 예상되는 시험결과
- 실제결과 : 시험절차를 실제로 수행하였을 때 나타나는 시험결과
- 예상결과와 실제결과의 비교 : 예상결과 및 실제결과를 비교한 결과

평가자는 시험서의 시험환경, 시험절차, 시험범위 분석, 상세설계 시험 등 시험의 타당성을 평가하였다. 평가자는 개발자의 시험 및 시험결과가 평가환경에 적합함을 검증하였다.

- **시험환경**

시험서에 서술된 시험환경은 시험을 위한 구성, 평가제품, TOE가 설치된 서버 또는 보안관제대상시스템 등 세부 환경을 포함하고 있다. 또한, 각 시험항목을 시험하기 위해 필요한 시험도구 등 세부적인 시험환경을 서술하고 있다.

- **시험범위 분석/상세설계 시험**

세부 평가결과는 ATE_COV 및 ATE_DPT 평가결과에 서술되어 있다.

- **시험결과**

시험서는 각 시험항목의 예상결과 및 실제결과를 서술하고 있다. 실제결과는 실제 제품의 동작화면 뿐만 아니라 감사기록을 통해서도 확인할 수 있다.

7.2 평가자 시험

평가자는 개발자 시험과 동일한 평가환경 및 평가도구를 사용하여 평가제품을 설치하고 개발자가 제공한 시험항목 전체를 시험하였다. 평가자는 모든 시험항목에서 실제결과가 예상결과와 일치함을 확인하였다.

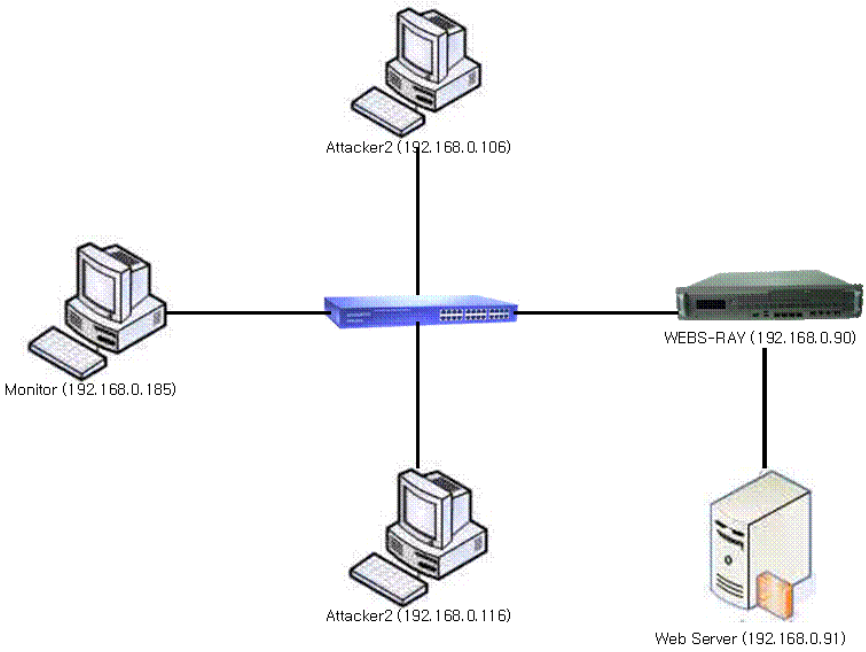
또한, 평가자는 개발자 시험에 기초하여 별도의 평가자 시험항목을 고안하여 시험한 결과, 실제결과가 예상결과와 일치함을 확인할 수 있었다.

평가자는 취약성 시험을 수행한 결과, 평가환경에서 어떠한 취약성도 악용 가능하지 않다는 점을 확인하였다.

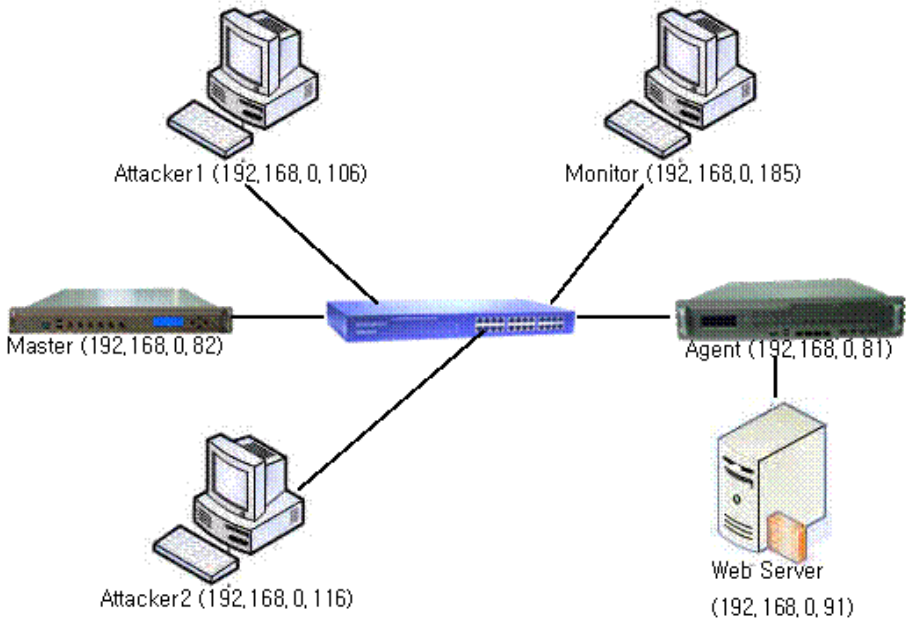
평가자의 시험결과는 평가제품이 설계문서에 서술된 대로 정상적으로 동작됨을 보증하였다.

8. 평가환경

평가자는 시험을 위해서 [ST]에서 명시된 환경구성과 일관성 있게 시험 환경을 구성하였다.



[그림 5] 평가자 시험환경(일체형)



[그림 6] 평가자 시험환경(분리형)

평가제품에서 제공하는 모든 보안기능이 평가범위에 포함되며, 각 보안기능의 세부적인 보안속성 및 환경설정 방법에 따라 평가환경을 구성하였다.

9. 평가결과

평가는 정보보호시스템 공통평가기준 V2.3, 정보보호시스템 공통평가방법론 V2.3을 적용하였다. 평가는 평가제품이 정보보호시스템 공통평가기준 2부, 정보보호시스템 공통평가기준 3부의 EAL4 평가보증등급 요구사항을 만족한다고 평가하였다. 자세한 평가결과는 평가보고서에 서술되어 있다.

- **보안목표명세서 평가 (ASE)**

평가자는 ASE 공통평가방법론 작업단위를 적용하여 평가하였다.

보안목표명세서 소개는 완벽하고 보안목표명세서의 다른 부분과 일관성이 있으며 보안목표명세서를 정확하게 식별하고 있다. TOE 설명은 TOE 목적 및 그 기능성을 이해할 수 있도록 설명하며, 조리 있고 완벽하며 내부적으로 일관성이 있으며, 보안목표명세서의 다른 부분과 일관성 있게 서술되어 있다.

보안환경은 TOE와 TOE 보안환경에서 유도된 명확하고 일관된 보안상의 문제를 가정사항, 위협, 조직의 보안정책으로 정의하여 제공하고 있으며, 완전하고 일관성 있게 서술되어 있다. 보안목적은 식별된 위협을 만족시키며 식별된 조직의 보안정책을 달성하며, 서술된 가정사항을 만족시키고 있다.

IT 보안요구사항은 완전하고 일관성 있게 서술되어 있으며, 보안목적을 달성하기 위한 TOE의 개발에 알맞은 기반을 제공하고 있다. TOE 요약명세는 보안기능과 보증척도를 정확하고 일관성 있게 정의하고, 서술된 TOE 보안요구사항을 만족하고 있다. 보안목표명세서는 수용하는 보호프로파일을 정확히 실체화하고 있다.

따라서, 보안목표명세서는 완전하고, 일관성 있고, 기술적으로 타당하며, 결과적으로 상응하는 TOE 평가의 기초자료로 사용하기에 적합하다.

- **형상관리 평가 (ACM)**

평가자는 ACM 공통평가방법론 작업단위를 적용하여 평가하였다. 형상관리 문서로부터 개발자가 구현 표현에 대한 수정을 위해 자동화 도구를 사용하여 통제하고 있음을 확인하였다. 형상관리 문서로부터 개발자가 TOE 및 TOE와 관련된 형상항목을 명확하게 식별하고 있으며, 이러한 항목들을 변경하는 능력은 적절히 통제됨을 확인하였다. 형상관리 문서로부터 개발자가 최소한 TOE 구현의 표현, ST의 보증 컴포넌트에서 요구하는 평가증거물, 보안 결함에 대하여 형상관리를 수행함을 확인하였다.

따라서, 형상관리 문서는 소비자가 평가된 TOE를 식별하도록 해주며, 형상항목이 유일하게 식별됨을 보장하고 개발자가 TOE 변경을 통제 및 추적하기 위해 사용한 절차가 적절함을 보장한다.

- **배포 및 운영 평가 (ADO)**

평가자는 ADO 공통평가방법론 작업단위를 적용하여 평가하였다. 배포 문서는 TOE를 사용자 측에 배포하는 경우 TOE의 보안을 유지하고 TOE의 변경 및 대체를 탐지하기 위한 모든 절차를 서술하고 있다. TOE의 안전한 설치, 생성 시동을 위한 절차 및 단계는 문서화되어 있으며, 그 결과 TOE는 안전하게 환경구성됨을 확인하였다.

따라서, 배포 및 운영 문서는 개발자가 의도한 방식과 동일하게 TOE가 설치, 생성, 시동되며, TOE가 변경되지 않고 배포됨을 보장하기에 적절하다.

- **개발 평가 (ADV)**

평가자는 ADV 공통평가방법론 작업단위를 적용하여 평가하였다. 기능명세는 TOE 보안기능을 적절히 서술하고 있으며, TOE 보안기능이 보안목표명세서의 보안기능요구사항을 만족시키기에 충분함을 설명하고 있다. 또한, TOE 외부 인터페이스를 적절하게 서술하고 있다. 보안정책모델은 보안정책의 규칙과 특징을 기술하는 데 명확하고 일관성이 있으며, 기능명세에 기술된 보안기능과 대응하도록 기술하고 있다.

기본설계는 TSF를 주요 구성 요소인 서브시스템으로 서술하고 있으며, 서브시스템의 인터페이스를 적절하게 서술하며, 기능명세를 정확하게 실현하고 있다. 상세설계는

TOE 보안기능의 내부 동작을 모듈과 모듈간의 상호관계 및 종속관계에 관하여 서술하고 있다. 상세설계는 보안목표명세서의 보안기능요구사항을 만족하기에 충분하며, 기본설계를 정확하고 효과적으로 정교화하고 있다.

구현의 표현은 보안목표명세서의 보안기능요구사항을 만족하기에 충분하며, 상세설계를 정확하게 실현하고 있다. 표현의 일치성은 개발자가 보안목표명세서의 요구사항을 기능명세, 기본설계, 상세설계, 구현의 표현으로 정확하게 완벽하게 구현했음을 보여준다.

따라서, 개발에서 TOE 외부 인터페이스를 설명하는 기능명세, TOE 구조를 내부 서브시스템으로 설명하는 기본설계, TOE 구조를 내부 모듈로 설명하는 상세설계, 소스코드 수준의 설명인 구현의 표현, 이러한 TOE 표현방법의 일관성을 보장하기 위해 서로 대응시키는 표현의 일치성 문서는 TOE 보안기능을 제공하는 방법을 이해하기에 적절하다.

- **설명서 평가 (AGD)**

평가자는 AGD 공통평가방법론 작업단위를 적용하여 평가하였다. 관리자설명서에는 관리자가 보안관리 인터페이스에 접속하는 방법과 보안관리 인터페이스에서 제공되는 각 메뉴에 대한 설명과 주의사항을 실례를 들어 서술하고 있다. 관리자설명서에서 서술된 내용이 정확하게 수행됨을 확인하였다.

- **생명주기 지원 평가 (ALC)**

평가자는 ALC 공통평가방법론 작업단위를 적용하여 평가하였다. 개발자의 개발환경에 대한 보안통제는 TOE를 안전하게 운영하기 위해 필요한 TOE 설계 및 구현의 비밀성 및 무결성을 제공하기에 적절함을 확인하였다. 개발자가 문서화된 TOE 생명주기 모델을 사용하고 있음을 확인하였다. 개발자가 일관성 있고 예측할 수 있는 결과를 낼 수 있는 잘 정의된 개발 도구를 사용했음을 확인하였다.

따라서, 생명주기 지원은 TOE 개발 전 과정에 사용된 보안절차 및 도구를 포함하여 TOE를 개발하고 유지보수하는 동안 개발자가 사용하는 절차를 적절하게 서술하고 있다.

- **시험 평가 (ATE)**

평가자는 ATE 공통평가방법론 작업단위를 적용하여 평가하였다. 시험서에는 보안목표명세서에 명시된 보안기능에 대해서 시험목적, 단계별 시험 절차 및 시험결과를 서술하고 결과를 예시하고 있다. 제공된 개발 과정별 기능시험과 모듈시험 등의 시험과정을 반복 수행하여 시험서에 서술된 시험 내용이 정확함을 확인하였으며 개발과정에서 구현된 보안기능의 동작이 일치함을 확인하였다. 또한 평가자 독립적인 시험을 수행하여 개발자 시험의 정확성을 확인하였다.

- **취약성 평가 (AVA)**

평가자는 AVA 공통평가방법론 작업단위를 적용하여 평가하였다. 오용 분석에서 설명서가 오해되지 않고 불합리하지 않으며 상충되지 않음을 확인하였으며, 모든 운영모드에 대한 안전한 절차가 다루어졌으며, 설명서를 사용하면 TOE의 불안전한 상태를 방지 및 탐지할 수 있음을 확인하였다. 기능강도 선언은 보안목표명세서의 모든 확률 및 순열 메커니즘에 대하여 선언되었으며, 개발자의 기능강도 선언에 대한 분석은 정확함을 확인하였다.

취약성 분석서에는 TOE에 대해서 명백하게 알려진 취약성과 이에 대한 대응책을 기능 구현 또는 지침서나 설명서에 운용환경을 명시하는 등 대응책을 적절하게 서술하고 있으며, 평가자가 독립적인 취약성 분석을 수행하여 취약성 분석의 정확성을 확인하였다. 취약성 분석에서 TOE는 의도된 환경 내에서 낮은 수준의 공격 수준을 가진 공격자에 의해 악용 가능한 취약성을 가지지 않음을 확인하였다.

따라서, 개발자 및 평가자의 취약성 분석 및 평가자의 침투시험에 기반하여 의도한 환경 내에서 TOE에 악용 가능한 결함 및 약점이 존재하지 않음을 확인하였다.

10. 권고사항

- 본 제품은 HTTP/HTTPS 프로토콜을 이용한 공격에 대해 탐지하고 차단할 수 있는 웹 어플리케이션 방화벽 제품으로 HTTP/HTTPS 이외의 프로토콜을 이용한 공격에 취약할 수 있다. 따라서, 본 평가제품의 보안효과를 높이기 위해 네트워크 앞단에 침입차단시스템, 침입방지시스템, 침입탐지시스템 등의 네트워크 보안제품을 설치 운영해야 한다.

- 본 제품은 웹 서버에서 정상적으로 동작되고 서비스되는 웹 문서를 수집/관리하는 WhiteURL 추가/삭제기능을 가지고 있으며, WhiteURL로 등록되어 있는 웹 문서는 외부에서 접근이 가능하다. 따라서, 중요 디렉토리 및 문서가 WhiteURL로 수집되어 관리되는 경우 악의적인 공격자에게 노출될 수 있으므로 WhiteURL 관리 대상 선정시 신중을 기해야 한다. 즉, 본 평가제품의 설치 운영시 WhiteURL 대상에 대한 선별 작업이 선행되어야 한다.

- 새로운 웹 관련 취약점 발생 시 웹 공격 탐지규칙 갱신을 위해 ㈜트리니티소프트에서는 본 평가제품에 대한 업데이트 룰을 제공하므로 관리자는 주기적으로 ㈜트리티니소프트 회사 홈페이지를 통해 업데이트 사항을 확인하여 최신 웹공격 탐지규칙을 유지해야 한다.

- 본 제품은 감사기록 저장공간 소진으로 임계치에 도달하는 경우 관리자 통보

기능을 제공하나 관리자는 통보 기능에만 의존하지 말고 지속적으로 저장공간 사용량을 점검하고 감사기록 저장공간을 확보해야 한다.

11. 약어 및 용어 정의

아래의 약어 및 용어가 본 보고서에서 사용되었다.

(1) 약어

CC 공통평가기준(Common Criteria)

EAL 평가보증등급(Evaluation Assurance Level)

PP 보호프로파일(Protection Profile)

ST 보안목표명세서(Security Target)

TOE 평가대상(Target of Evaluation)

(2) 용어

TOE	평가의 대상인 IT제품이나 시스템 및 이와 관련된 설명서
감사기록	TOE의 보안에 관련된 사건의 기록을 저장하는 감사데이터
사용자	TOE 외부에서 TOE와 상호 동작하는 모든 실체, 사용자, 외부 IT 실체 등
인가된 관리자	TOE 보안정책에 따라 TOE를 안전하게 관리하는 인가된 사용자로 설치자, 슈퍼관리자, 관리자, 모니터 계정이 존재
외부 IT 실체	TOE 외부에서 TOE와 상호 작용하는 안전하거나 안전하지 않은 모든 IT 제품이나 시스템
WhiteURL	웹 서버에서 정상적으로 동작되고 서비스 되는 페이지를 등록하는 것을 White URL 수집이라고 부르며 수집된 파일들을 White URL이라고 함
웹 어플리케이션 방화벽	웹 서버 또는 웹 어플리케이션의 취약성을 이용한 공격을 탐지하고 차단하기 위하여 HTTP/HTTPS 패킷을 감사하고 흐름을 통제하는 정보보호제품

12. 참고문헌

인증기관은 아래의 문서를 사용하여 본 인증보고서를 작성하였다:

[1] 정보보호시스템 공통평가기준 V2.3(2008. 7. 16.)

[2] 정보보호시스템 공통평가방법론 V2.3

[3] 정보보호시스템 평가·인증 지침 (2008. 7. 16.)

[4] 정보보호제품 평가인증 수행규정 (2008. 9. 1.)

[5] WEBS-RAY V2.5 보안목표명세서 V2.8 (2008. 11. 3.)

[6] WEBS-RAY V2.5 평가결과보고서, 발행버전 1.0 (2008. 12. 5.)